UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/857,218	06/22/2001	Ryuji Ishiguro	209462	6422

22850 7590 12/29/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/857,218	ISHIGURO ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,11-29,38-44 and 50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,11-29,38-44 and 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/11/2005 has been entered.

Response to Arguments

2. In response to communications filed on 10/11/2005, applicant amends claims 1, 11, 21, 22, 38, 39, and 50; cancels claims 6-10, 30-37, and 45-49. The following claims 1-5, 11-29, 38-44 and 50 are presented for examination.

2.1 The amendments to overcome the claim objections have been considered, and the 112 rejection to claims 39 and 45 has been withdrawn.

2.2 Applicant's arguments, pages 14-22, filed on 10/11/2005, with respect to the rejection of claims 1-50 have been fully considered but they are moot in view of a new ground of rejection. Applicant has amended the claims to replace a storage medium by a compact disc. Zhang discloses a compact disc to store encrypted contents data (column 7, lines 15-30 and 45-51). Sims further discloses accessing encrypted content data from a CD using a content key. Upon further consideration the independent claims are now rejected in view of Zhang and Sims.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 1, 11, and 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Claims 1, 11, and 21 recite "before said contents is transmitted/received". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-5, 11-22, 25-29, 38-44, and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,550,008 to **Zhang et al** in view of US Patent Publication US 2002/0016919 to **Sims, III**.

4.2 **As per claims 11, 22, 38, Zhang et al** discloses a method for furnishing key data to a data processing apparatus, furnishing a first key to said data processing apparatus on which a contents reproducing program is installed, for example (see column 3, lines 45-65 and column 11, lines 28-35; see also column 15, line 45 through column 16, line 12) for software installation; said first key data to acquire contents data stored in an external recording medium for storage such as compact disc (column 7, lines 15-30 and 45-51) in said data processing apparatus, said first key data also being used in authentication for transmission/reception of said contents data with a portable reproducing apparatus connected to said data processing apparatus, for example (see column 6, line 60 through column 8; column 4, line 37 through column 5, line 19; column 5, line 50 through column 6, line 35); if said portable reproducing apparatus and the program reproducing program from said data processing apparatus effects transmission/reception of contents data distributed from said contents server, second key data different from said first key data is furnished over a network, for example (see column 8, line 44-67); and wherein said second key data is used for acquiring contents data furnished from said contents server for storage in said data processing apparatus, said second key data also being used for authentication of said data processing apparatus and said portable reproducing apparatus in order to effect transmission/reception of the contents data from said contents server, for example (see column 10, line 10-55; column 8, line 44 through column 9, line 30). **Zhang et al** discloses

authentication is performed before the content is transmitted (see column 12, lines 48-67); **Zhang et al** also discloses the limitations of claim 11 in other embodiment throughout the invention, for example in columns 11-14. Although the invention discloses key derivation for acquiring the content using a shared key, **Zhang et al** suggests that the invention is not limited to a specific crypto scheme, for example (see column 2, lines 12-48 and column 4, lines 20-36). **Zhang et al** also suggests in another embodiment two different sets of key data furnished by a server one for authentication and another for encryption of content, for example (see column 12, lines 8-22). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the invention of **Zhang et al** to use public/private key scheme for encrypting the data instead of generating symmetric key data in the device as public/private key provides more security. It is also very well known in the art the use of key pair including a public key for authentication and a private key for encryption as disclosed for example by Schneier in "Applied Cryptography" . Therefore these modifications would have been obvious to any one skilled in the art of cryptography without departing from the spirit and scope of the invention as suggested by **Zhang et al**. **Zhang et al** teaches encrypted contents data received from the head end can be stored in an external recording medium for storage such as a compact disc (see column 7, lines 15-30 and 44-51) also discloses the POD decrypting content data received from a provider according to key access protocol (column 3, lines 25-44), but was silent about the POD retrieving the data from the storage element (CD) because it is obvious that if the data is stored in the CD it must be retrieved using a key. It is apparent to one skilled in the art that a content key may be used to access the data from the storage element. **Sims, III** in an analogous art discloses media content protection wherein a content provider sends content key

and authentication keys the content is accessed from a media device using a disk key or content key (page 8, paragraph 81 and page 9, paragraph 98) and discloses to execute the content a public key (authentication key) and content key are needed (page 6, paragraphs 54-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to restrict access to the media by using a key to acquire the content, as taught by **Sims, III** (page 9, paragraph 98). One skilled in the art would have been motivated to do so because it would add security to the content and at the same time ensures that only authorized devices are allowed to use the encrypted content as suggested by **Sims, III** (page 9, paragraph 98).

As per claims 1, 17, 21, Zhang et al substantially teaches at least three devices: a content server, POD module (any device connected to a host or integrated circuit device, etc.) that meets the recitation of data processor and a host device (any device that has a receiver such as a video cassette recorder, personal computer etc.) that meets the recitation of portable reproducing device, for example (see column 3, lines 1-35); it is understood that they could be interchanged, and further discloses that the devices are not limited to the examples and the invention is not limited to television broadcast system but any other system including other audio/video transmission using means such as the Internet etc., for example (see column 2, lines 49-67). **Zhang et al** also discloses transmission of keys for authentication and content protection that meets the recitation of first master and authentication key, for example (see column 15, line 30 through column 16, line 12 and column 12, lines 8-22). **Zhang et al** also discloses second set of keys different from the first keys for authentication between the first and the second device.

Although the invention discloses key derivation for acquiring the content, the invention is not limited to a specific crypto scheme, for example (see column 2, lines 12-48 and column 4, lines 20-36). In one embodiment **Zhang et al** discloses second key sets with at least two keys for authentication and transmission/reception of the contents data, for example (see column 4, line 20 through column 5, line 30). Claims 1 and 6 recite the same inventive concept as claim 11 except for using a master key and authentication key for each key set, and as discussed above the use of a master key and authentication key for each key set does not depart from the spirit and scope of the invention disclosed by **Zhang et al.** Therefore, claims 1, 6, 17, 21 are rejected on the same rationale as the rejection of claims 11, 21, 22, 30, 38.

As per claims 16 and 42, Zhang et al discloses the limitation of using key data for decrypting the content received from a content server that meets the recitation of wherein said second key is a server connecting key for downloading contents from a contents server, for example (see column 10, lines 10-30).

As per claims 18-20 and 25-27, Zhang et al discloses the limitation of wherein said first key data is furnished from an external storage medium, for example (see column 4, line 37 through column 5, line 19; column 5, line 50 through column 6, line 35).

As per claims 2, 13, 29, 44, Zhang et al substantially teaches updating keys, for example (see column 2, lines 42-48) and substantially teaches the limitation of wherein the portable device holds authentication keys and master keys and keys being furnished to reproducing

program over the network and further teaches said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation as discussed above. **Zhang et al** does not explicitly teach the reproducing device holding first to i'th authentication keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger. However, **Sims, III** in an analogous art discloses a portable reproducing device holding generations of keys, for example (see page 9, paragraphs 0093-0097; page 10, paragraphs 0107-0108; page 13, claims 22-23). **Sims, III** further discloses that by having a list of authorized keys and updating means this invention not only provides protection, but also provides limited access of content. For instance, list of authorized keys may be updated by communication with an external source to allow a media device to securely provide content key to a decoder not originally included as an authorized decoder, for example (see page 3, paragraph 0022), in addition media devices may be allowed to generate their own protected content. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to provide a reproducing device holding generation of keys, as taught by **Sims, III**. The motivation to do so is given by **Sims, III** because by having a list of authorized keys and updating means the invention as combined would not only provide protection, but also provide limited access of content; list of authorized keys may be updated by communication with an external source to allow a media device to securely provide content key to a decoder not originally included as an authorized decoder, for example (see page 3, paragraph 0022), in addition media devices may be allowed to generate their own protected content as suggested by **Sims, III**.

Claims 3-5, and 43, recite the same inventive concept as claim 2 and therefore they are rejected on the same rationale as the rejection of claims 2 7, 13, 44, 49 above.

As per claims 12, 14, 28, 39, 40, and 50, these claims recite similar limitations as found in claims 2 and 11, except for using ID information and key data of plural generations. **Zhang et al** discloses the limitation of using ID to generate and update new key data that meets the recitation of wherein the ID information of said portable reproducing apparatus and key data of an ith generation are transmitted to said data processing apparatus and wherein the generation of key data of said portable reproducing apparatus is updated based on the ID information of said portable reproducing apparatus, for example (see column 9, lines 1-50; and column 8). **Sims, III** further discloses storing key data of plural generations therefore these claims are rejected on the same rationale as the rejection of claims 2 and 11.

As per claims 15 and 41, Zhang et al discloses the limitation of using a compact disk for storage and processor for using key data for accessing the content that meets the recitation of wherein the first key is a ripping key for ripping contents from a compact disc, for example (see column 7, lines 1-30).

5. **Claims 23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,550,008 to **Zhang et al** in view of US Patent Publication US 2002/0016919 to **Sims, III** as applied to claim 22 and further in view of US Patent 6,751,598 to **Yagawa et al**.

5.1 **As per claims 23-24, Zhang et al** discloses installing the application and routines from an external storage to perform the copyright control of the invention that meets the recitation of wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium, for example (see column 10, lines 10-30). **Yagawa et al** in an analogous art discloses wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium and also discloses wherein key data is settled at the same time as said comprehensive management unit is installed in order to prevent an illegal copy from being distributed, which meets the recitation of wherein key data for the 0th generation as said first key data is acquired at the same time as said comprehensive management unit is installed, , for example (see column 6, line 30 through column 7, line 46; column 12, lines 4-18; see also column 11, lines 1-35 for processing copyright management using user ID and key data). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to have key data for the 0th generation as said first key data acquired at the same time as said comprehensive management unit is installed, in order to prevent an illegal copy of the digital content from being distributed, as taught by **Yagawa et al**. One skilled in the art would have been motivated to do so as suggested by **Yagawa et al** so as to prevent tampering during installation and to prevent illegal copy of the digital content from being distributed, for example (see column 7, lines 19-46).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses some of the claim features.

US Patents: US2004/0117644 Colvin; 5,987,607 Tsumura.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
December 22, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100